

CLAIMS

What is claimed is:

5 1. A method for recording a verifiable messaging session , said method comprising the steps of:

recording a selection of message entries from a messaging session, wherein a plurality of users are participating in said messaging session; and

10 attaching a plurality of digital signatures each separately associated with one from among said plurality of users to said recording of said selection of message entries from said messaging session, such that the messaging session is verifiable.

15 2. The method for recording a verifiable messaging session according to claim 1, said method further comprising the step of:

recording said selection of message entries and attaching said plurality of digital signatures at a messaging server system communicatively connected via a network to a plurality of client 20 systems accessible to said plurality of users.

25 3. The method for recording a verifiable messaging session according to claim 1, said method further comprising the step of:

recording said selection of message entries and attaching said plurality of digital signatures at a client system communicatively connected via a network to a plurality of client systems accessible to said plurality of users.

4. The method for recording a verifiable messaging session according to claim 1, said method further comprising the step of:

5 verifying said messaging session, wherein verifying includes at least one of verifying at least one of said plurality of digital signatures and verifying an integrity of said messaging session.

5. The method for recording a verifiable messaging session according to claim 1, said method further comprising the step of:

10 transmitting a request to said plurality of users to each attach a digital signature to said recording of said selection of message entries from said messaging session.

6. The method for recording a verifiable messaging session according to claim 1, said method further comprising the step of:

15 storing a plurality of keys each associated with one from among said plurality of digital signatures such that said plurality of keys are accessible to said plurality of users for verifying said plurality of digital signatures.

7. The method for recording a verifiable messaging session according to claim 1, said step of attaching a plurality of digital signatures further comprising the steps of:

5 calculating a checksum for said recording of said selection of message entries from said messaging session; and

10 encrypting said checksum utilizing a private key for a particular digital signature from among said plurality of digital signatures, wherein a particular public key is enabled to decrypt said encrypted checksum.

15 8. The method for recording a verifiable messaging session according to claim 7, said method further comprising the step of:

20 15 verifying an integrity of said selection of said plurality of message entries by:

25 calculating a current checksum for said selection of said plurality of message entries;

decrypting said encrypted checksum with said particular public key; and

25 comparing said current checksum with said decrypted checksum, wherein said integrity is verified if said decrypted checksum matches said current checksum.

9. The method for recording a verifiable messaging session according to claim 1, said method further comprising the step of:

verifying a particular digital signature from among said plurality of digital signatures in order to verify a particular user from among said plurality of users associated with said particular digital signature.

10. The method for recording a verifiable messaging session according to claim 9, said step of verifying a particular digital signature from among a plurality of digital signatures, further comprising the steps of:

determining whether a public key received in order to verify said particular digital signature matches a public key coupled to said particular digital signature; and

in response to determining a match, verifying said particular user associated with said particular digital signature.

11. A system for recording a verifiable messaging session, said system comprising:

a server system communicatively connected to a network;

5

· said server system further comprising:

means for recording a selection of message entries from a messaging session, wherein a plurality of users are 10 participating in said messaging session; and

means for attaching a plurality of digital signatures each separately associated with one from among said plurality of users to said recording of said selection of message entries from said messaging session, such that the messaging session is verifiable.

12. The system for recording a verifiable messaging session according to claim 11, said system further comprising:

20 a logging controller for verifying said messaging session, wherein said verifying includes at least one of verifying at least one of said plurality of digital signatures and verifying an integrity of said messaging session.

25

13. The system for recording a verifiable messaging session according to claim 11, said system further comprising:

means for transmitting a request to said plurality of users to each attach a digital signature to said recording of said selection of message entries from said messaging session.

14. The system for recording a verifiable messaging session according to claim 11, said system further comprising:

10 a log file repository for storing a plurality of public keys each associated with one from among said plurality of digital signatures such that said plurality of public keys are accessible to said plurality of users for verifying said messaging session.

15. The system for recording a verifiable messaging session according to claim 11, said means for attaching a plurality of digital signatures further comprising:

20 means for calculating a checksum for said recording of said selection of message entries from said messaging session; and

means for encrypting said checksum utilizing a private key for a particular digital signature from among said plurality of digital signatures, wherein a particular public key is enabled to 25 decrypt said encrypted checksum.

16. The system for recording a verifiable messaging session according to claim 15, said system further comprising:

means for verifying an integrity of said selection of said plurality of message entries by:

5 calculating a current checksum for said selection of said plurality of message entries;

10 decrypting said encrypted checksum with said particular public key; and

15 comparing said current checksum with said decrypted checksum, wherein said integrity is verified if said decrypted checksum matches said current checksum.

17. The system for recording a verifiable messaging session according to claim 11, said system further comprising:

20 means for verifying a particular digital signature from among said plurality of digital signatures in order to verify a particular user from among said plurality of users associated with said particular digital signature.

18. The system for recording a verifiable messaging session according to claim 17, said means for verifying a particular digital signature from among a plurality of digital signatures, further comprising:

5

means for determining whether a public key received in order to verify said particular digital signature matches a public key coupled to said particular digital signature; and

10

means for verifying said particular user associated with said particular digital signature, in response to determining a match.

15

19. A program for recording a verifiable messaging session, residing on a computer usable medium having computer readable program code means, said program comprising:

20

means for enabling recording of a selection of message entries from a messaging session, wherein a plurality of users are participating in said messaging session; and

25

means for attaching a plurality of digital signatures each separately associated with one from among said plurality of users to said recording of said selection of message entries from said messaging session, such that the messaging session is verifiable.

20. The program for recording a verifiable messaging session according to claim 19, said program further comprising:

means for enabling verification of said messaging session,
5 wherein verifying includes at least one of verifying at least one of said plurality of digital signatures and verifying an integrity of said messaging session.

21. The program for recording a verifiable messaging session according to claim 19, said program further comprising:

means for controlling transmission of a request to said plurality of users to each attach a digital signature to said recording of said selection of message entries from said messaging session.

22. The program for recording a verifiable messaging session according to claim 19, said program further comprising:

means for enabling storage of a plurality of keys each associated with one from among said plurality of digital signatures such that said plurality of keys are accessible to said plurality of users for verifying said plurality of digital signatures.

23. The program for recording a verifiable messaging session according to claim 19, said means for attaching a plurality of digital signatures further comprising:

5 means for calculating a checksum for said recording of said selection of message entries from said messaging session; and

10 means for enabling encryption of said checksum utilizing a private key for a particular digital signature from among said plurality of digital signatures, wherein a particular public key is enabled to decrypt said encrypted checksum.

15 24. The program for recording a verifiable messaging session according to claim 23, said program further comprising:

means for verifying an integrity of said selection of said plurality of message entries by:

20 calculating a current checksum for said selection of said plurality of message entries;

decrypting said encrypted checksum with said particular public key; and

25 comparing said current checksum with said decrypted checksum, wherein said integrity is verified if said decrypted checksum matches said current checksum.

25. The program for recording a verifiable messaging session according to claim 19, said program further comprising:

means for verifying a particular digital signature from
5 among said plurality of digital signatures in order to verify a particular user from among said plurality of users associated with said particular digital signature.

26. The program for recording a verifiable messaging session
10 according to claim 25, said program further comprising:

means for determining whether a public key received in order to verify said particular digital signature matches a public key coupled to said particular digital signature; and

15 means for verifying said particular user associated with said particular digital signature, in response to determining a match.

10
15
20

27. A method for transmitting verifiable message entries in a messaging session, said method comprising the steps of:

5 attaching a digital signature for a sender of a message entry to said message entry; and

10 distributing said message entry to a plurality of participants in a messaging session, wherein each of said plurality of participants in said messaging session are enabled to verify said message entry with said digital signature in real-time.

15 28. The method for transmitting verifiable message entries according to claim 27, said method further comprising the step of:

56 attaching said digital signature for said sender at a client messaging system before distribution within a network.

20 29. The method for transmitting verifiable message entries according to claim 27, said method further comprising the step of:

25 attaching said digital signature for said sender at a messaging server before distribution to said plurality of participants.

30. The method for transmitting verifiable message entries according to claim 27, said method further comprising the step of:

5 verifying at least one of an identity of said sender and an integrity of content of said message entry.

31. A system for transmitting verifiable message entries in a messaging session, said system comprising:

10 a messaging system communicatively connected to a network;

15 said messaging system further comprising:

means for attaching a digital signature for a sender of a message entry to said message entry; and

20 means for distributing said message entry to a plurality of participants in a messaging session, wherein each of said plurality of participants in said messaging session are enabled to verify said message entry with said digital signature in real-time.

25 32. The system for transmitting verifiable message entries according to claim 31, said system further comprising:

means for attaching said digital signature for said sender at a client messaging system before distribution within a network.

33. The system for transmitting verifiable message entries according to claim 31, said system further comprising:

means for attaching said digital signature for said sender at a messaging server before distribution to said plurality of participants.

34. The system for transmitting verifiable message entries according to claim 31, said system further comprising:

means for verifying at least one of an identity of said sender and an integrity of content of said message entry.

35. A program for transmitting verifiable message entries in a messaging session, residing on a computer usable medium having computer readable program code means, said program comprising:

means for enabling attachment of a digital signature for a sender of a message entry to said message entry; and

means for controlling distribution of said message entry to a plurality of participants in a messaging session, wherein each of said plurality of participants in said messaging session are enabled to verify said message entry with said digital signature in real-time.

36. The program for transmitting verifiable message entries according to claim 35, said program further comprising:

means for enabling attachment of said digital signature for
5 said sender at a client messaging system before distribution
within a network.

37. The program for transmitting verifiable message entries according to claim 35, said program further comprising:

10 means for enabling attachment of said digital signature for
said sender at a messaging server before distribution to said
plurality of participants.

15 means for verifying at least one of an identity of said
sender and an integrity of content of said message entry.

20